CLAIMS

What is claimed is:

1. A method for acquiring public-key infrastructure (PKI) credentials for a user, the method comprising:

generating a pre-registration record for the user;

sending the pre-registration record as an e-mail attachment in an e-mail message to the user at a client;

generating at the client a cryptographic key pair comprising a user private key and a user public key;

sending a PKI credential request for the PKI credentials to a certificate issuing authority, wherein the public key certificate request comprises the pre-registration record and the user public key; and

receiving the PKI credentials at the client.

2. The method of claim 1 further comprising:

retrieving user information from a directory; and

storing the user information into the pre-registration record.

3. The method of claim 1 further comprising:

viewing the e-mail message within a browser, wherein the browser generates the cryptographic key pair; and

storing the user private key in a secure local keystore at the client by the browser.

4. The method of claim 1 wherein the e-mail message is formatted according to an Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

5. The method of claim 1 further comprising:

prompting the user for user authentication data to be included in an attribute certificate; and

storing the user authentication data in the PKI credential request.

6. The method of claim 1 further comprising:

retrieving a Uniform Resource Identifier (URI) from the e-mail message; and

posting the public key certificate request to the certificate issuing authority using the URI.

7. The method of claim 1 further comprising:

storing the PKI credentials in a secure local keystore at the client.

8. The method of claim 1 wherein the PKI credentials comprise a public key certificate for the user and an attribute certificate for the user.

9. The method of claim 1 further comprising:

publishing the PKI credentials in a directory.

10. The method of claim 1 wherein the PKI credentials are formatted according to an X.509 standard.

11. An apparatus for acquiring public-key infrastructure (PKI) credentials for a user, the apparatus comprising:

means for generating a pre-registration record for the user;

means for sending the pre-registration record as an e-mail attachment in an e-mail message to the user at a client;

means for generating at the client a cryptographic key pair comprising a user private key and a user public key;

means for sending a PKI credential request for the PKI credentials to a certificate issuing authority, wherein the public key certificate request comprises the pre-registration record and the user public key; and

means for receiving the PKI credentials at the client.

12. The apparatus of claim 11 further comprising:

means for retrieving user information from a directory; and

means for storing the user information into the pre-registration record.

13. The apparatus of claim 11 further comprising:

means for viewing the e-mail message within a browser, wherein the browser generates the cryptographic key pair; and

means for storing the user private key in a secure local keystore at the client by the browser.

14. The apparatus of claim 11 wherein the e-mail message is formatted according to an Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

15. The apparatus of claim 11 further comprising:

means for prompting the user for user authentication data to be included in an attribute certificate; and

means for storing the user authentication data in the PKI credential request.

16. The apparatus of claim 11 further comprising:

means for retrieving a Uniform Resource Identifier (URI) from the e-mail message; and

means for posting the public key certificate request to the certificate issuing authority using the URI.

17. The apparatus of claim 11 further comprising:

means for storing the PKI credentials in a secure local keystore at the client.

18. The apparatus of claim 11 wherein the PKI credentials comprise a public key certificate for the user and an attribute certificate for the user.

19. The apparatus of claim 11 further comprising:

means for publishing the PKI credentials in a directory.

20. The apparatus of claim 11 wherein the PKI credentials are formatted according to an X.509 standard.

21. A computer program product in a computer-readable medium for use in a data processing system for acquiring public-key infrastructure (PKI) credentials for a user, the computer program product comprising:

instructions for generating a pre-registration record for the user;

instructions for sending the pre-registration record as an e-mail attachment in an e-mail message to the user at a client;

instructions for generating at the client a cryptographic key pair comprising a user private key and a user public key;

instructions for sending a PKI credential request for the PKI credentials to a certificate issuing authority, wherein the public key certificate request comprises the pre-registration record and the user public key; and

instructions for receiving the PKI credentials at the client.

22. The computer program product of claim 21 further comprising:

instructions for retrieving user information from a directory; and

instructions for storing the user information into the pre-registration record.

23. The computer program product of claim 21 further comprising:

instructions for viewing the e-mail message within a browser, wherein the browser generates the cryptographic key pair; and

instructions for storing the user private key in a secure local keystore at the client by the browser.

24. The computer program product of claim 21 wherein the e-mail message is formatted according to an Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

25. The computer program product of claim 21 further comprising:

instructions for prompting the user for user authentication data to be included in an attribute certificate; and

instructions for storing the user authentication data in the PKI credential request.

26. The computer program product of claim 21 further comprising:

instructions for retrieving a Uniform Resource Identifier (URI) from the e-mail message; and

instructions for posting the public key certificate request to the certificate issuing authority using the URI.

27. The computer program product of claim 21 further comprising:

instructions for storing the PKI credentials in a secure local keystore at the client.

28. The computer program product of claim 21 wherein the PKI credentials comprise a public key certificate for the user and an attribute certificate for the user.

29. The computer program product of claim 21 further comprising:

instructions for publishing the PKI credentials in a directory.

30. The computer program product of claim 21 wherein the PKI credentials are formatted according to an X.509 standard.